FILED
NOV 27 2018
CLERK, U.S. DISTRICT COURT
ALEXANDRIA, VIRGINIA

IN THE UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA	Case No. 1:18-MJ-557
v.	**Filed Under Seal**
THOMAS ANDREW LARETTO,	
Defendant.	

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT AND ARREST WARRANT

I, Raymond Abruzzese, being duly sworn, depose and state:

INTRODUCTION

1. I have been employed as a Special Agent of the U.S. Department of Homeland Security (DHS), Homeland Security Investigations (HSI) since in or around March 2003, and am currently assigned to Child Exploitation Unit in Dulles, Virginia.

2. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography, as well as commercial fraud and immigration fraud. I have gained experience through everyday work relating to conducting these types of investigations. I also have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography, as defined in 18 U.S.C. § 2256(8), including computer media. Due to my experience and training, I can identify child pornography when I see it. I have training and experience in the enforcement of the laws of the United States, including the

preparation, presentation, and service of subpoenas, affidavits, criminal complaints, search warrants, and arrest warrants.

3. This Affidavit is made in support of a criminal complaint and arrest warrant charging **THOMAS ANDREW LARETTO** with knowingly receiving child pornography in violation of Title 18, U.S. Code, Sections 2252(a)(2) and (b)(1).

4. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted, along with my conversations with law enforcement officers and others and the review of reports, database records, and other materials. This Affidavit is submitted for the limited purpose of supporting a criminal complaint and securing an arrest warrant. It does not include each and every fact known to me or the government about the investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that **LARETTO** knowingly received child pornography.

BACKGROUND TO PEER-TO-PEER FILE SHARING, EMULE, AND THE EDONKEY NETWORK

5. Peer-to-peer (P2P) file sharing is a method of communication available to Internet users through the use of software downloaded from the Internet. It is used to share digital files between different users of a P2P network. The hallmark of P2P file sharing is that users of a particular P2P network upload and download files to and from one another's computers, as opposed to a centralized server. The availability of a particular file on a P2P network at any given time thus depends on whether any other users are connected to the network and making that file available. One such P2P file sharing application is named "eMule," and it operates using the "eDonkey" network, both of which are discussed further below.

6. Law enforcement agencies have compiled databases of known files containing child pornography that are checked against files being distributed over P2P networks. For the

eMule program used by law enforcement, this list is known as a "Files of Interest" list. The "Files of Interest" list contains files that have been previously viewed by law enforcement officers and determined to contain suspected child pornography.

7. The eDonkey2000, or "eDonkey," network is one of several P2P file-sharing networks on the Internet. It can be accessed by computers running many different client programs. These programs share common protocols for network access and file sharing. The user interface, features, and configuration may vary between clients and versions of the same client.

8. eMule is one such P2P client, or file sharing application, on the eDonkey network. In my training and experience, I have learned that eMule is an open-source software program that is available for free on the Internet. The eMule software allows users to conduct keyword searches for files that are shared on the eDonkey network. When a keyword search is started, the search is sent out over a worldwide network of computers using compatible P2P software. The results of the keyword search are displayed to the user. The user then selects a file or files to be downloaded from the displayed results. A file that is downloaded by the user is stored in the area of the user's computer that was selected by the user and remains there until moved or deleted by the user.

9. The eDonkey network's file-sharing capability is based on the eDonkey hash algorithm. This mathematical algorithm allows for the unique identification of files. The eDonkey hash algorithm is calculated by first dividing each file into 9,728,000 byte parts. The Message-Digest 4 (MD4) hash algorithm is then applied to each file part, starting with Part 0. The MD4 hash algorithm is then applied to the sequential concatenation of the MD4 hashes applied to each file part, thereby creating the unique eD2k hash value. If the file size is less than

9,728,000 bytes, then the eD2k hash of the file is equivalent to the MD4 hash. The MD4 hash is a 128-bit algorithm typically represented as 32-digit hexadecimal numbers. The eDonkey Hash is called "secure" because it is computationally infeasible for two files with different content to have the same eDonkey hash value.

10. I know the following facts about the eDonkey network and eMule software based on my training and experience, as well as from discussions with other trained law enforcement officers:

a. The eDonkey network is frequently used in the online trading of child pornography. It is used to trade digital files including still images and movie files of child pornography.

b. When eMule software is first installed on a computer, a unique 16-byte identifier is generated for the software user, referred to as the "User Hash." Unless the user deletes his or her "User Hash," this hash value remains the same for every use by that user of the eMule software on that computer. In eMule, this value is generally stored on the user's computer in a file named "preferences.dat," which is located in the configuration directory.

c. During the installation of eMule, which requires the user to provide a "shared" folder, various settings are established that configure the host computer to share—*i.e.*, distribute—files. For each file located in a user's shared directory, eMule processes the file and computes an eDonkey hash value.

d. Users of the eDonkey network may receive a selected file from numerous sources by accepting segments of the file from multiple users and then reassembling the complete file on the local computer. The network uses eDonkey hash values to ensure that exact copies of the same file are used during this process.

e. When a user connects to the eDonkey network, a list of shared files, descriptive information, and their associated eDonkey hash values are made searchable to allow other computers on the eDonkey network to search for and locate these files.

11. Law enforcement has modified the standard eMule software to only allow the downloading of a single file from a single IP address, as well as the displaying of additional information about the source file and the source user.

DETAILS OF THE INVESTIGATION

12. In or around October 2015, an HSI undercover agent began an investigation of a subject who was using the Internet Protocol (IP) address 108.56.132.136 (hereinafter, the "Target IP") to access the Internet and use eMule P2P software to receive and distribute images of child pornography.

13. During the course of the investigation into the Target IP, the HSI undercover officer was able to make a direct connection with the Target IP via eMule P2P software and downloaded video files. For instance, on or about October 22, 2015, the HSI undercover officer downloaded a complete video file from the Target IP with an eD2K hash value of 5DF46D73138BB0A26B0DCE4E646F6424. A review of the downloaded file indicates that it was entitled "Brother and sisters webcam suck_some good shots.avi," was approximately 8 minutes and 1 second in length, and depicted two female minors and one male minor performing sexually explicit acts on one another, such as one of the female minors performing fellatio on the other female minor, one of the female minors touching the other's vagina, and one of the female minors performing oral sex on the male minor.

14. Thereafter, HSI obtained records from Verizon Fios regarding the Target IP. According to those records, at the time that the video file described above was downloaded from

the Target IP, the Target IP was assigned to **LARETTO** at a residential address in Reston, which is within Fairfax County, Virginia, in the Eastern District of Virginia (hereinafter, the "Laretto Residence"). A check of publically available property records indicates that **LARETTO** is the sole owner of the Laretto Residence and has been since at least October 2015.

14. Based on the foregoing events and information, a search warrant for the Laretto Residence was sought from the Commonwealth of Virginia. This search warrant was sought based upon violations of Virginia Code § 18.2-374.1:1 ("Possession, reproduction, distribution, and facilitation of child pornography; penalty"), which at the time stated, in relevant part:

> Any person who knowingly possesses child pornography is guilty of a Class 6 felony. . . .
>
> Any person who knowingly . . . reproduces by any means, including by computer, sells, gives away, distributes, electronically transmits, displays, purchases, or possesses with intent to sell, give away, distribute, transmit, or display child pornography . . . shall be punished by not less than five years nor more than 20 years in a state correctional facility.

On or about January 4, 2016, a Commonwealth of Virginia magistrate approved and issued the requested search warrant for the Laretto Residence.

A. Execution of the Virginia State Search Warrant

16. On or about January 7, 2016, HSI and other Virginia law enforcement officers executed the Virginia state search warrant at the Laretto Residence. **LARETTO** was the only occupant of the Laretto Residence at the time of the search warrant execution.

17. A number of electronic devices were seized during the search, including: a black generic computer tower (S/N 5VP8Z3MW); a red Western Digital (WD) My Passport external hard drive (S/N WX61C12N4500); and a WD 2TB external hard drive (S/N WXK1A9141668). The black computer tower was located in an upstairs bedroom, while the WD My Passport

external hard drive and the WD 2TB external hard drive were located on a television stand near one of **LARETTO**'s televisions. All of the electronic devices seized have been maintained in DHS/HSI's custody.

18. During the execution of this search warrant, an HSI Special Agent and a Fairfax County Police Detective conducted a voluntary interview with **LARETTO**, which resulted in the following statements and admissions:

a. **LARETTO** stated that he was the owner of the Laretto Residence and stated that he had been the only person living at the residence for the past few months. He also stated that he works in the information technology field for an area company.

b. **LARETTO** admitted that he used eMule and that there was child pornography on some of his electronic devices. He added that "upstairs" in his residence law enforcement would find a computer, which he described as being a self-built computer, containing child pornography. **LARETTO** also provided a password for this device.

c. Additionally, **LARETTO** admitted that there was a red Western Digital external drive underneath a television that also contained child pornography and that this is the device he used to store the pornography he downloads.

d. **LARETTO** stated that he had a "good bit" of child pornography that he had accumulated over the past four years. He added that he had been using eMule for two years, and acknowledged knowing how the file sharing system worked and that he knew other people could potentially obtain images and videos from him. **LARETTO** stated he attempted to minimize the sharing of files by moving the files out of his download folder, explaining that his goal was not to share the child pornography files, but rather just to watch them.

e. **LARETTO** also stated he would get aroused and masturbate while watching the images and videos he downloaded.

21. On or about March 26, 2018, out of an abundance of caution, a federal search and seizure warrant was obtained from the U.S. District Court for the Eastern District of Virginia for the devices being held in DHS/HSI custody to include the black generic computer tower, the red WD My Passport external hard drive, and the WD 2TB external hard drive, all of which are discussed above.

B. The Forensic Analysis of the Computer Tower

22. A forensic analysis of the previously identified black generic computer tower revealed that this device contained approximately 71 videos of child pornography, to include what appear to be prepubescent children engaged in sexual activity with themselves, other children, and adults. The images of child pornography located on the device include both minor males and females ranging from preschool through early teenage years, and some of these images depict bondage and bestiality. The following are examples of files that depict child pornography located on the computer tower:

a. A video file entitled "1st studio – Siberian Mouse - M 33 Promo (Masha-Ina-Kriss Lesbian Oral Sex).wmv," which was located within the file path "\Users\Tom\Desktop\fav" and depicts three, nude prepubescent females engaging in sexually explicit conduct to include one of the prepubescent females conducting oral sex on one of the other prepubescent females.

b. A video file entitled "[1st Studio] Siberian Mouse HD_127," which was located within the file path "\Users\Tom\Desktop\Siberian Mouse," and depicts two prepubescent females engaging in sexually explicit conduct to include one of the prepubescent females inserting a device into the other female's vagina.

c. A video file entitled "1st Studio – Siberian Mouse – MSH-45 Cumshot HQ," which was located within the file path "\Users\Tom\Desktop\Siberian Mouse," and depicts an up-close image of a minor female's face and an adult male's erect penis, which the adult male is masturbating and eventually ejaculates into the minor female's mouth.

23. Also located on the computer tower was the P2P Software program "eMule," which was installed on or about October 1, 2011. A file folder was located at the file path "\Users\Tom\AppData\Local\eMule\config," and this folder contains configuration information about the eMule program, including the following:

a. One particular file that was identified was entitled "known.met," which contains information about shared files and files currently in the process of being downloaded. A review of the file names that are contained within the known.met file includes files that have names that I know through my training and experience are indicative of or likely to depict child pornography to include: (i) "(Thai Pthc) (優先) Thai Pthc 2009 Lollipop 1-01B (Milla 11Yo And Suzi 8Yo,2009).avi"; (ii) "Thai Pthc 2009 Lollipop-Issue#2-3.avi"; (iii) "Thai Pthc 2009 Lollipop-issue#2-2.avi"; and (iv) "Thai Pthc 2009 Lollipop Issue 1-03A (Milla 11yo and Suzi 8 yo).avi." I know that "pthc" and "yo" are common child pornography acronyms; to wit: "pthc" is short for "pre-teen hardcore" and "yo" is short for "years old."

b. Another configuration file that was located was entitled "AC_SearchStrings.dat." This file contains search terms entered by the computer user while using the eMule program. A review of the searched keywords contained in the AC_SearchStrings.dat file revealed terms I know through my training and experience are associated with child pornography such as "lollipop" and "Siberian Mouse."

24. I know that Microsoft Internet Explorer is a program included with the Microsoft Windows operating system used to access web sites on the Internet as well as files stored locally on the computer. Internet Explorer activity observed during the forensic review of the computer tower revealed a folder within "Users\Tom\AppData\Local\Microsoft\Windows\WebCache." Contained within the "WebCache" folder was a file entitled "WebCacheV01.dat," which lists Internet Explorer activity from on or about January 29, 2012 through January 7, 2016. A review of this Internet Explorer activity indicates that from on or about March 12, 2014, to October 18, 2015, hundreds of images and videos containing file titles that I know from my training and experience to be indicative of or likely to contain child pornography were accessed. Additionally, law enforcement cross referenced a smaller number of the file titles with content found elsewhere on **LARETTO's** devices and found files with matching titles that did depict child pornography. This Internet Explorer activity includes entries from on or about April 22, 2014, during which Windows user "Tom" accessed email and programs relating to **LARETTO's** employer both hours before and after viewing videos with titles indicative of child pornography, some of which match videos of child pornography found elsewhere on **LARETTO's** devices. Similarly, on or about March 4, 2014, websites associated with **LARETTO's** employer were accessed within ten minutes of the computer tower being used to view a video matching the file title of child pornography content found elsewhere on **LARETTO's** devices.

25. Another type of forensic artifact for which I have training and experience is Jump Lists, which also are known as Automatic Destinations and Custom Destinations. This forensic artifact is a feature of the Windows operating system designed to provide Windows users with quick access to recently opened files for specific applications in the Windows Task Bar. Automatic Destinations are created by the operating system when the user performs an action

such as opening a file or playing a video, whereas Custom Destinations are created when the user manually pins a file to the application in the Task Bar. I also know that the operating system creates a separate Jump List file for each program used by the computer user. With respect to the computer tower, it was determined that the folder located at "\Users\Tom\AppData\Roaming\Microsoft\Windows\Recent" contains information about images and videos accessed by the computer user. A list of videos viewed by the computer user include numerous file names that I know from my training and experience are indicative of child pornography. Some examples of these video titles are: (a) "stickam\lesb\Pthc- Lesbian Lolitas - ((Hussyfan)) Mylola-Stasia Sveta6.mpeg"; and (b) "Prev Tab\Ped\lesb\10yo Lesbians.mpg."

26. In addition, I know from my training and experience that a forensic artifact similar to Jump Lists are LNK files. Windows automatically creates LNK files when a user views or access images, videos, and files on the computer. For the computer tower, the forensic review uncovered LNK files associated with file names that, in my training and experience, are indicative of child pornography, such as: (a) "Childlover_little_Collection_Video_0075.mpeg"; (b) "9yo & 10yo 69 (les).mpeg"; (c) "Thai Pthc 2009 Lollipop-issue#2-2.avi"; and (d) "Thai Pthc 2009 Lollipop Issue 1-03A (Milla 11yo and Suzi 8yo)." Markedly, example (c) matches the name of a file associated with the use of eMule as described in subparagraph 23(a) of this Affidavit.

27. In addition to the information summarized above, there is further reason to believe that the computer tower is owned and controlled by **LARETTO**. This is because the forensic review identified a number of documents and files on the computer tower associated with **LARETTO**, such as PDFs and Word documents with his name in the title of the document, as well as a bank statement for one of **LARETTO's** accounts.

C. The Forensic Analysis of the WD External Drives

28. A forensic analysis of the red WD My Passport external hard drive also was conducted, and that review revealed that the device contained at least 200 videos of child pornography, including what appear to be prepubescent children engaged in sexual activity with themselves, other children, and adults. For instance, one of the videos founds on the device was within the file path "\Downizzloads\n:" and was entitled "!New!(Ptch)Veronika 2Young Girls Lesb 100.avi." This video depicts two nude prepubescent females, one of whom performs oral sex on the other's vagina.

29. A forensic review of the 2TB WD external hard drive was conducted, too, and it revealed at least 114 videos of child pornography. One of the file folders located on this WD external hard drive was within a file path called "eMule\Incoming," and it contained videos of child pornography, such as a file entitled "Brother and sisters webcam suck, some good shots.avi," which appears to be the same, or at least extremely similar, as the file that was downloaded by the HSI undercover agent from the Target IP, as discussed above in Paragraph 13. According to the forensic analysis, this file has a modified date of May 26, 2015, which is prior to the date that HSI conducted the undercover downloaded from the Target IP.

//

//

//

//

//

//

//

CONCLUSION

30. For the foregoing reasons, I submit to the Court that probable cause exists to believe that **THOMAS ANDREW LARETTO** has knowingly received child pornography in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1). I, therefore, respectfully request that the Court issue a criminal complaint and arrest warrant authorizing the arrest of **LARETTO**.

Respectfully submitted,

Special Agent Raymond Abruzzese
Homeland Security Investigations

Subscribed to and sworn to before me
on this 27th day of November, 2018.

/s/
Ivan D. Davis
United States Magistrate Judge